XRayWatch

...and you see EVERYTHING

itWatch

itWatch GmbH
Stresemannstr. 36
D-81547 Munich

Tel.: +49 (0) 89 / 62 03 01 00
Fax: +49 (0) 89 / 69 39 28 04

XRayWatch@itWatch.de
www.itWatch.de

XRayWatch – Simply See EVERYTHING

Closing of Data Leaks

A memory stick with a certain serial number has been granted to a specific user. But can you control what data the user is exchanging with that device? **XRayWatch** protects company confidential information against data theft. **XRayWatch** protects the company network against hostile or unauthorised data contents, i.e. malicious code or embedded executables.

Proactive Protection against the Forbidden

Your company secrets should not be stored on memory sticks - readable for everyone? You do not want users to import or execute software or portable apps from a portable medium on thin or fat clients? **XRayWatch** defines who may read which data with which application from where and who may export it to what target-network shares, local hard drives or portable devices.

Log the Permitted

Users read and change information. Prohibitions constrain the day-to-day business. For sensitive information a conservation of evidence is important: Who patched the Login.exe of a board member work station with a Trojan Horse? Who read the contents of an ad-hoc message for the stock exchange before the publication and took it along? **XRayWatch** quickly and efficiently helps you to answer these urging questions.

XRayWatch controls the file access of all users according to centrally defined guidelines. The user and application rights are defined on network shares, local directories or portable devices, i.e. USB sticks, CD/DVDs, cameras etc. - a clear and useful guideline can be defined in a few minutes. Because of the fact that the file names may be misleading, XRayWatch also enforces a detailed content control (pattern match) of all files and the detailed monitoring of all activities. Together with PDWatch the customer is able to define which data require encryption.

- Not only file names but also file contents are checked by pattern matching
- A general company guideline can be refined to any level based on White and Black List. Both White and Black Lists are supported for content and file names.

- Who may read or write which files on which portable device?
- The customers can extend or modify the pattern matching rules themselves

…and much more at www.itWatch.info

Check Contents - Not File Names

Companies check the content and file names of exchanged data with their firewalls and mail-gateways. Why only there and not on the broadband interfaces of the PCs? Clever users already know to change file names. With its semantic and syntactic Pattern Matching **XRayWatch** offers a detailed check of all exchanged data at all ports and interfaces – the re-naming of the file is no threat.

Company Guidelines are Individual

Executable programs may be embedded in Word documents. Is that supposed to be? Best if the costumer decides! Obviously, confidential Word documents should not be treated in the same way as publicly accessible documents. **XRayWatch** allows a Pattern Check that can be optionally extended or modified by our customer – “MyCompany confidential“ in the header of the file can be one of the defined criteria which can prevent the take along of those files or at least the unencrypted export.

Compliance

Data Protection Acts require special protection measures for the storing of personal data to portable media. With **XRayWatch** you are able to identify personal data and to block its export or enforce an encryption with **PDWatch**.

Locale Safe

Information that needs special protection can be stored in the Local Safe of the local hard drives. With **XRayWatch** you can control which data go in and out of the safe: proactively blocked, logged or encrypted. The user can only access the local safe with special trustworthy programs – the customer defines these programs. **PDWatch** and **XRayWatch** enable the implementation of very complex requirements in the areas of **Endpoint Security** and **Information Leakage Prevention**.

FSXRW-081016en